sciendo

uniform distribution theory

DOI: 10.2478/UDT-2021-0008
Unif. Distrib. Theory **16** (2021), no.2, 71–88

DIVISIBILITY PARAMETERS AND THE DEGREE OF KUMMER EXTENSIONS OF NUMBER FIELDS

Antonella Perucca — Pietro Sgobba — Sebastiano Tronto

Department of Mathematics, Faculty of Science, Technology and Medicine,
University of Luxembourg, LUXEMBOURG

ABSTRACT. Let K be a number field, and let ℓ be a prime number. Fix some elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a subgroup of $K^\times$ of rank r. Let $n_1, \dots, n_r$, m be positive integers with $m \geqslant n_i$ for every i. We show that there exist computable parametric formulas (involving only a finite case distinction) to express the degree of the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ over $K(\zeta_{\ell^m})$ for all $n_1, \dots, n_r, m$. This is achieved with a new method with respect to a previous work, namely we determine explicit formulas for the divisibility parameters which come into play.

1. Introduction

Let K be a number field, and let ℓ be a prime number. Fix some elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a (without loss of generality) torsion-free subgroup of $K^\times$ of rank r. Since this is a natural question in Kummer theory, we are interested in computing the degree of the Kummer extension

$$K\big(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\big)/K(\zeta_{\ell^m}) \tag{1}$$

for all positive integers $n_1, \dots, n_r, m$ with $m \geqslant n_i$ for every i, where ζ_{ℓ^m} denotes a primitive ℓ^mth root of unity. In a recent work [4] we have proven that it is

2010 Mathematics Subject Classification: Primary: 11Y40; Secondary: 11R20, 11R21.
Keywords: number field, Kummer theory, Kummer extension, degree.

possible to compute parametric formulas (involving only a finite case distinction) to express the degree of the extensions (1) for *all* $n_1, \dots, n_r, m$. We now achieve this result in a more direct way. Namely, setting $n = \max(n_1, \dots, n_r)$ we can write the above extension as

$$K\Big(\zeta_{\ell^m},\ \sqrt[\ell^n]{\alpha_1^{\ell^{n-n_1}}}, \dots,\ \sqrt[\ell^n]{\alpha_r^{\ell^{n-n_r}}}\Big)/K(\zeta_{\ell^m})\,. \tag{2}$$

By the results in [1, Section 3.3], the degree of this extension is known to depend only on certain finitely many computable divisibility parameters for the group

$$\left\langle \alpha_1^{\ell^{n-n_1}}, \dots,\ \alpha_r^{\ell^{n-n_r}} \right\rangle. \tag{3}$$

So we want to determine these divisibility parameters as $n_1, \dots, n_r$ vary.

More precisely, given a finitely generated and torsion-free subgroup G of $K^\times$ of positive rank r, we consider two types of parameters expressing the ℓ-divisibility of G in K: the d-parameters are non-negative integers $d_1, \dots, d_r$, while the h-parameters are non-negative integers $h_1, \dots, h_r$ that can be at most the ℓ-adic valuation of $\#\mu_K$, where μ_K is the group of roots of unity in K. We formally define these notions, as well as the notion of strongly ℓ-independent elements, in Section 2.

The main result we achieve is the following (see Theorem 4.4).

Theorem 1.1. *Let K be a number field, and let ℓ be a prime number. Fix some elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank r. There is a finite procedure to determine formulas for the ℓ-divisibility parameters of the group*

$$\left\langle \alpha_1^{\ell^{x_1}}, \dots,\ \alpha_r^{\ell^{x_r}} \right\rangle \tag{4}$$

for all non-negative integers $x_1, \dots, x_r$. There is a finite partition of the set of r-tuples $x_1, \dots, x_r$ such that, if we restrict to any subset of the partition, the d-parameters d_i are such that $\delta_i := d_i - x_i$ are fixed integers, where $i \in \{1, \dots, r\}$, and the corresponding h-parameters are fixed integers ε_i.

We also prove various assertions for the ℓ-divisibility parameters of the groups (4) and for the degrees of the Kummer extensions (1). In particular, we prove the following result, where v_ℓ denotes the ℓ-adic valuation over $\mathbb{Q}$.

Theorem 1.2. *Let K be a number field, and let ℓ be a prime number such that $\ell \neq 2$ or $\zeta_4 \in K$. Let ω be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^\omega})$. Fix some elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank r. Then for all $n_1, \dots, n_r, m$ with $m \geq n := \max_i(n_i)$ and $m \geq \omega$*

we have

$$v_\ell\big[K\big(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\sqrt[\ell^{n_r}]{\alpha_r}\big) : K(\zeta_{\ell^m})\big] = \max\big\{0, n-m+\varepsilon_i-\max(n_i-\delta_i,0) : 1\le i\le r\big\} + \sum_{i=1}^{r}\max(n_i-\delta_i,0),$$

where $\delta_1,\dots,\delta_r$ and $\varepsilon_1,\dots,\varepsilon_r$ are as in Theorem 1.1 (setting $x_i := n-n_i$).

In Section 5 we explain how we can compute the degrees of the Kummer extensions (1) in the case $\ell = 2$ and $\zeta_4 \notin K$. More precisely, we describe how the 2-divisibility parameters of a group of the form (4) in $K^\times$ change from K to $K(\zeta_4)$. Finally, in Section 6, we provide explicit formulas for the ℓ-divisibility parameters of a torsion-free subgroup of $K^\times$ of rank at most 3.

As an aside remark, notice that it is possible to consider the degree of

$$K\big(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\sqrt[\ell^{n_r}]{\alpha_r}\big)$$

also over K, because cyclotomic degrees are easy to compute. For the same reason we could suppose without loss of generality that the elements $\alpha_1,\dots,\alpha_r$ generate a torsion-free subgroup of $K^\times$.

2. Divisibility parameters

Let K be a number field, and let ℓ be a prime number. Let μ_K be the group of roots of unity in K and define $z := v_\ell(\#\mu_K)$, where v_ℓ is the ℓ-adic valuation over $\mathbb{Q}$. If ζ is a root of unity, then we denote by $\operatorname{ord}(\zeta)$ its order.

An element $a \in K^\times$ is called *strongly ℓ-indivisible* if there is no root of unity ζ in K (whose order we may suppose to be a power of ℓ) such that ζa is an ℓth power in $K^\times$. We call $a_1,\dots,a_r \in K^\times$ *strongly ℓ-independent* if $a_1^{x_1}\cdots a_r^{x_r}$ is strongly ℓ-indivisible whenever $x_1,\dots,x_r$ are integers not all divisible by ℓ.

Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. If $g_1,\dots,g_r$ is a basis of G as a free $\mathbb{Z}$-module, then we can write

$$g_i = \xi_i \cdot b_i^{\ell^{d_i}}$$

for some strongly ℓ-indivisible elements $b_i \in K^\times$, for some integers $d_i \ge 0$, and for some $\xi_i \in \mu_K$ of order ℓ^{h_i}. We call d_i and h_i the ℓ-divisibility parameters of g_i, and we call b_i the *strongly ℓ-indivisible part* of g_i. In general, b_i and h_i may depend on the chosen decomposition: if $h_i \le z - d_i$, then there is another decomposition for which $h_i = 0$; if $h_i > z - d_i$, then h_i is unique.

We call $g_1, \dots, g_r$ an *ℓ-good basis* of G if $b_1, \dots, b_r$ are strongly ℓ-independent or, equivalently, if the sum $\sum_i d_i$ is maximal among the possible bases of G, see [1, Section 3.1]. In this case, we call d_i and h_i the *d-parameters* and *h-parameters* for the ℓ-divisibility of G in K. The d-parameters of G are unique up to reordering, while in general the h-parameters are not unique (one may require additional conditions as to make them unique, see Remark 3). Recall from [1, Theorem 14] that an ℓ-good basis of G always exists, and from [1, Section 6.1] that the ℓ-divisibility parameters are computable.

Lemma 2.1. *Let $A_1, \dots, A_r$ be elements of $K^\times$ which are strongly ℓ-independent. Then for all non-zero integers $X_1, \dots, X_r$ and for every ℓ^zth root of unity ζ, the element $\zeta \prod_{i=1}^r A_i^{X_i}$ has d-parameter $\min_i\big(v_\ell(X_i)\big)$ and h-parameter $v_\ell\big(\mathrm{ord}(\zeta)\big)$.*

Proof. Set $d := \min_i\big(v_\ell(X_i)\big)$. The element

$$A := \prod_{i=1}^r A_i^{X_i/\ell^d}$$

is the product of powers of strongly ℓ-independent elements whose exponents are not all divisible by ℓ and hence it is strongly ℓ-indivisible. So we can write

$$\zeta \prod_{i=1}^r A_i^{X_i} = \zeta A^{\ell^d}$$

and from the latter decomposition we can easily read off the ℓ-divisibility parameters. □

Lemma 2.2 ([1, Corollary 16])**.** *The d-parameters $d_1, \dots, d_r$ for G are such that for every sufficiently large integer n we have*

$$\frac{G}{G \cap (K^\times)^{\ell^n}} \cong \bigoplus_{i=1}^r \frac{\mathbb{Z}}{\ell^{n-d_i}\mathbb{Z}}\,.$$

Remark 1. If H is a subgroup of G of finite index, then the d-parameters for H are greater than or equal to the d-parameters for G. More precisely, if

$$d_1, \dots, d_r \qquad \text{and} \qquad d'_1, \dots, d'_r$$

are the d-parameters (ordered non-decreasingly) for G and H, then we have

$$d_i \le d'_i \qquad \text{for all} \qquad i \in \{1, \dots, r\}.$$

Indeed, if n is sufficiently large, then we have

$$\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{\ell^{n-d'_i}\mathbb{Z}} \cong \frac{H}{H \cap (K^\times)^{\ell^n}} \hookrightarrow \frac{G}{G \cap (K^\times)^{\ell^n}} \cong \bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{\ell^{n-d_i}\mathbb{Z}}$$

considering that the group homomorphism

$$H \hookrightarrow G/G \cap (K^\times)^{\ell^n} \quad \text{has kernel} \quad H \cap (K^\times)^{\ell^n}.$$

If m is an integer coprime to ℓ, then clearly the groups G and G^m have the same ℓ-divisibility parameters. This observation and Remark 1 give

Remark 2. If H is a subgroup of G of index coprime to ℓ, then the d-parameters for H are the same as those for G.

Remark 3. Let d_i with $i \in \{1, \dots, r\}$ be the d-parameters of G, ordered non-decreasingly. By [1, Appendix] the corresponding h-parameters h_i, for an appropriate choice of the ℓ-good basis of G, satisfy the following conditions (which mean that the h-parameters are taken zero whenever possible) and in this case the multiset of the pairs (d_i, h_i) is unique:

(1) For every $1 \leqslant i \leqslant r$ we have $h_i = 0$ or $h_i > z - d_i$.

(2) If $1 \leqslant i < j \leqslant r$ and $h_i, h_j > 0$ hold, then we have $h_i > h_j$ and $d_i + h_i < d_j + h_j$.

(3) If $1 \leqslant i < j \leqslant r$ and $d_i = d_j$ hold, then $h_j = 0$.

To obtain an ℓ-good basis as above there is provided an algorithm in [1, Proposition 31].

3. An intrinsic description for the h-parameters

Let K be a number field, let ℓ be a prime number, and let G be a torsion-free and finitely generated subgroup of $K^\times$ of positive rank r.

Remark 4. If H is a subgroup of G of finite index, then it is not true, in general, that the h-parameters (as in Remark 3) do not increase from G to H. For example, let a_1, a_2 be strongly ℓ-independent elements of $K^\times$, and let $n \geq 1$, $z \geq 2$: considering

$$G := \left\langle a_1^{\ell^n},\, \zeta_{\ell^z} a_2^{\ell^{z+n}} \right\rangle \qquad H := \left\langle \zeta_{\ell^z} \left(a_1 a_2^{\ell^z}\right)^{\ell^n}, \zeta_{\ell^{z-1}} a_2^{\ell^{z+n+1}} \right\rangle$$

the h-parameters of G are $(0, z)$, whereas the h-parameters of H are $(z, z-1)$.

However, in general we have the following property.

Lemma 3.1. *Let H be a subgroup of G of finite index, and let $h_1, \dots, h_r$ (respectively, $h'_1, \dots, h'_r$) be the h-parameters as in Remark 3 for G (respectively, H). Then for every $i \in \{1, \dots, r\}$ we have $h_i = 0$ or $h'_i \le h_i$.*

Proof. Let $g_1, \dots, g_r$ and $\gamma_1, \dots, \gamma_r$ be ℓ-good bases for G and H, respectively, such that their d-parameters d_i's and d'_i's are ordered non-decreasingly and their h-parameters h_i's and h'_i's satisfy the conditions of Remark 3. There are integers e_{ij}, roots of unity $\xi_j \in \mu_K$ of order ℓ^{h_j}, and strongly ℓ-independent elements $b_j \in K^\times$ such that for every $i \in \{1, \dots, r\}$ we can write

$$\gamma_i = \prod_{j=1}^{r} g_j^{e_{ij}} = \prod_{j=1}^{r} \xi_j^{e_{ij}} \cdot b_j^{e_{ij}\ell^{d_j}} .$$

Suppose that h_i, h'_i are both strictly positive for some index i. Then $h'_i > z - d'_i$ and it does not depend on the decomposition, so we have $h'_i = v_\ell\big(\operatorname{ord} \prod_j \xi_j^{e_{ij}}\big)$. To prove that this number is at most h_i, we show that $h_j - v_\ell(e_{ij}) < h_i$ for all $j \neq i$ with $h_j \neq 0$ and $e_{ij} \neq 0$. By Condition (2) of Remark 3 we have: if $j > i$, then $h_j < h_i$; If $j < i$, then $h_j + d_j < h_i + d_i$, and we conclude because $v_\ell(e_{ij}) + d_j \ge d'_i \ge d_i$ by Lemma 2.1 and Remark 1. □

We can prove a stronger property if we consider a subgroup of G of index coprime to ℓ.

Theorem 3.2. *If H is a subgroup of G of index coprime to ℓ, then the h-parameters (as in Remark 3) are the same for H and for G.*

Proof. Let m be the index of H in G. By Remark 2 the d-parameters d_i (in non-decreasing order) are the same for G, H, and G^m. Call h_i the corresponding h-parameters (as in Remark 3) for G, which are the same for G^m, and call h'_i the h-parameters for H. By Lemma 3.1 (applied once to G, H and once to H, G^m) we know that if h_i, h'_i are both non-zero, then $h_i = h'_i$. It suffices to show that $h'_i = 0$ implies $h_i = 0$ because the other implication can be proven analogously (replacing G, H by H, G^m). So suppose that $h'_i = 0$ and $h_i > 0$ for some index i.

We keep the notation of the proof of Lemma 3.1. We claim that there is some index s such that $d_s = d_i$ (hence $h'_s = 0$) and $v_\ell(e_{si}) = 0$. Since $\operatorname{ord} \xi_i^{e_{si}} = \ell^{h_i}$, by reasoning as in Lemma 3.1 we deduce that

$$v_\ell\left(\operatorname{ord} \prod_{j=1}^{r} \xi_j^{e_{sj}}\right) = h_i .$$

This is impossible because $h_i > z - d_i = z - d_s$ while the left-hand side is a possible h-parameter for γ_s so it is at most $z - d_s$.

To prove the claim, consider the matrix (e_{ij}), which has determinant coprime to ℓ, and decompose it in blocks by grouping together indices for which the d--parameters are the same. By Lemma 2.1 we have either $e_{ij} = 0$ or $v_\ell(e_{ij}) \geq d_i$, and in particular the blocks below the main diagonal are zero modulo ℓ. Then each square block on the main diagonal has determinant coprime to ℓ and the claim follows. □

4. The algorithm for the divisibility parameters

Let K be a number field, and let ℓ be a prime number. Fix some $\zeta \in \mu_K$ of order ℓ^z. Let

$$G := \langle g_1, \dots, g_r \rangle$$

be a torsion-free subgroup of $K^\times$ of positive rank r. Choosing an ℓ-good basis for G and considering the ℓ-indivisible parts of the elements of this basis, we find strongly ℓ-independent elements $b_1, \dots, b_r$ of $K^\times$ such that for all $i \in \{1, \dots, r\}$ we have

$$g_i := \zeta^{f_i} \cdot \prod_{j=1}^{r} b_j^{e_{ij}}, \tag{5}$$

where e_{ij} and f_i are integers, the matrix (e_{ij}) has rank r, and $1 \leq f_i \leq \ell^z$.

Lemma 4.1. *Suppose that for every $i, j \in \{1, \dots, r\}$ we have: $e_{ij} = 0$ for all $j < i$; $e_{ii} \neq 0$; $v_\ell(e_{ii}) = \min_{j \geq i}\big(v_\ell(e_{ij})\big)$ (where we restrict to the indices such that $e_{ij} \neq 0$). Then the g_i's are an ℓ-good basis of G.*

Proof. By Lemma 2.1 the strongly ℓ-indivisible part of g_i is

$$B_i := \prod_{j \geq i} b_j^{e_{ij} \ell^{-v_\ell(e_{ii})}}.$$

To prove that the B_i's are strongly ℓ-independent, suppose that $\xi \prod_i B_i^{z_i}$ is an ℓth power in $K^\times$ for some integers z_i and for some $\xi \in \mu_K$, and write

$$\prod_i B_i^{z_i} = \prod_j b_j^{n_j}, \qquad \text{where} \qquad n_j := \sum_{i \leq j} e_{ij} \ell^{-v_\ell(e_{ii})} z_i .$$

Since the b_j's are strongly ℓ-independent, we have $\ell \mid n_j$ for every j. In particular, since ℓ divides n_1 but not $e_{11}\ell^{-v_\ell(e_{11})}$, we have $\ell \mid z_1$, and then by iteration we deduce that $\ell \mid z_i$ for all i. □

Lemma 4.2. *The smallest d-parameter for G is the minimum of $v_\ell(e_{ij})$ (where we restrict to the indices such that $e_{ij} \neq 0$).*

Proof. Let $m := v_\ell(e_{i_0 j_0})$ be this minimum. Then all elements of G are ℓ^mth powers in $K^\times$ up to a root of unity, and hence every d-parameter is at least m. By Lemma 2.1 the d-parameter of g_{i_0} equals m, so not all d-parameters are greater than m. □

For every r-tuple $X = (x_1, \dots, x_r)$ of non-negative integers define the subgroup

$$H_X := \left\langle g_1^{\ell^{x_1}}, \dots, g_r^{\ell^{x_r}} \right\rangle$$

of G, which is again torsion-free and of rank r.

If $x_i + v_\ell(f_i) \geq z$ for every i, then by Lemma 2.1 the h-parameters of the elements $g_i^{\ell^{x_i}}$'s are zero and hence we can take the h-parameters of H_X to be all zero.

Remark 5. If the g_i's are an ℓ-good basis of G, then the $g_i^{\ell^{x_i}}$'s are an ℓ-good basis for H_X. So by Lemma 2.1 the group H_X has d-parameters $d_i = \min_j\big(v_\ell(e_{ij}) + x_i\big)$ (where we restrict to the indices such that $e_{ij} \neq 0$) and corresponding h-parameters $h_i = \max\big(0, z - x_i - v_\ell(f_i)\big)$.

From now on we order tuples of integers of the same length in lexicographic order.

Definition 4.3. Given the $(r + r^2 + r)$-tuple (x_i, e_{ij}, f_i), we consider a permutation σ_I on the the indices i and a permutation σ_J of the indices j and we define

$$\sigma(x_i, e_{ij}, f_i) = \left(x_{\sigma_I(i)}, e_{\sigma_I(i)\sigma_J(j)}, f_{\sigma_I(i)}\right).$$

For every $k \in \{1, \dots, r\}$ we define the following k^2-tuple (ordered according to (a, b))

$$\sigma_k(e_{ij}) := \left(e_{\sigma_I^{-1}(a)\sigma_J^{-1}(b)}\right) \qquad a, b \in \{1, \dots, k\}.$$

We similarly define the $(k^2 + k)$-tuple $\sigma_k(e_{ij}, f_i)$.

Theorem 4.4. *There is a finite procedure to determine ℓ-divisibility parameters of H_X for all X. The parameters only depend on the $(r+r^2+r)$-tuple (x_i, e_{ij}, f_i) (and the d-parameters do not depend on f_i).*

There is a permutation σ as in Definition 4.3 (which depends only on the $(r + r^2)$-tuple (x_i, e_{ij})), and for every $k \in \{1, \dots, r\}$ there are two functions δ_k and ϵ_k (which depend only on k, and which only involve sums, differences, products, and the ℓ-adic valuation) such that

$$d_k := x_{\sigma_I^{-1}(k)} + \delta_k\big(\sigma_k(e_{ij})\big) \qquad \text{and} \qquad h_k := \max\Big(0, z - x_{\sigma_I^{-1}(k)} - \epsilon_k\big(\sigma_k(e_{ij}, f_i)\big)\Big)$$

are ℓ-divisibility parameters of H_X, with $d_1, \dots, d_r$ in non-decreasing order. The above formulas for all X involve a finite case distinction, which means (considering the e_{ij} as fixed) partitioning the set of r-tuples X according to σ.

We can choose the functions δ_k in such a way that we can determine σ as follows. We determine $\big(\sigma_I^{-1}(k), \sigma_J^{-1}(k)\big)$ for all k. For $k = 1$, we choose the smallest pair of indices (for which δ_1 is well-defined) minimizing d_1. For $k > 1$ we consider the formula for d_k (where we have already fixed $\big(\sigma_I^{-1}(i), \sigma_J^{-1}(i)\big)$ for all $i < k$) and select indices from the remaining ones: we choose the smallest pair of indices (for which δ_k is well-defined) minimizing d_k.

The proof of the theorem outlines what we can choose as functions δ_k and ϵ_k. The fact that δ_k is not well-defined for all integer values of the variables is only due to the fact that the function involves the ℓ-adic valuation and we do not admit the expression $v_\ell(0)$. Expressions for δ_k and ϵ_k for k up to 3 can be found in Section 6.

Remark 6. The algorithm in the proof of the theorem transforms the augmented matrix $(e_{ij}\ell^{x_i} \mid f_i\ell^{x_i})$ into a matrix $(E_{ij} \mid F_i)$, where the square submatrix (E_{ij}) is upper-triangular. The d-parameters of H_X (in non-decreasing order) are $v_\ell(E_{ii})$, and the corresponding h-parameters are $v_\ell(\operatorname{ord}\zeta^{F_i})$. The finite case distinction yielding σ arises from the fact that we permute rows and columns of the matrix to work with entries having least ℓ-adic valuation (among a subset of the non-zero entries).

Proof. Consider the $r \times (r+1)$ integer matrix $(e_{ij}\ell^{x_i} \mid f_i\ell^{x_i})$, and notice that this matrix without the last column has rank r.

Step 1. Suppose that $e_{11}\ell^{x_1}$ is non-zero and has minimal ℓ-adic valuation among the non-zero entries of the first r columns. Then

$$d_1 := v_\ell(e_{11}\ell^{x_1}) = x_1 + v_\ell(e_{11}),$$

$$h_1 := v_\ell\Big(\operatorname{ord}\big(\zeta^{f_1\ell^{x_1}}\big)\Big) = \max\big(0, z - x_1 - v_\ell(f_1)\big)$$

are the smallest d-parameter of H_X (by Lemma 4.2) and a corresponding h--parameter (by the meaning of the last column).

If the above assumption is not satisfied, let (i_1, j_1) be the smallest pair of indices with $i_1, j_1 \in \{1, \dots, r\}$ such that $e_{i_1 j_1}\ell^{x_{i_1}}$ is non-zero and has minimal ℓ-adic valuation. Then we swap the rows $1, i_1$ and the columns $1, j_1$ and rename the indices according to these swaps.

Set $y := \ell^{-v_\ell(e_{11})}$. We multiply all rows $i \geq 2$ by $e_{11}y$, which corresponds to replacing H_X with a subgroup H'_X of index coprime to ℓ. Next, for each $i \geq 2$ we subtract a suitable integer multiple (namely, $ye_{i1}\ell^{x_i - x_1}$) of row 1 from row i, in such a way that the entry $(i,1)$ of the matrix becomes zero. This corresponds to a base change for the group H'_X. We obtain the matrix

$$\left(\begin{array}{cccc|c} e_{11}\ell^{x_1} & e_{12}\ell^{x_1} & \cdots & e_{1r}\ell^{x_1} & f_1\ell^{x_1} \\ 0 & y\Delta_{22}\ell^{x_2} & \cdots & y\Delta_{2r}\ell^{x_2} & y(e_{11}f_2 - e_{21}f_1)\ell^{x_2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & y\Delta_{r2}\ell^{x_r} & \cdots & y\Delta_{rr}\ell^{x_r} & y(e_{11}f_r - e_{r1}f_1)\ell^{x_r} \end{array}\right)$$

where

$$\Delta_{ij} = e_{11}e_{ij} - e_{i1}e_{1j}.$$

For $i \in \{2, \ldots, r\}$ and $j \in \{2, \ldots, r+1\}$, the (i,j) entry only depends on

$$e_{11}, e_{i1}, e_{1j}, e_{ij}, f_1, f_i, x_i$$

(and we can remove f_i from the above list if $j \neq r+1$).

Step 2. Let $X_2 = (x_2, \ldots, x_r)$. The submatrix obtained by deleting the first row and the first column corresponds to a torsion-free subgroup

$$H_{X_2} \text{ of } \langle b_2, \ldots, b_r, \mu_{\ell^z} \rangle \quad \text{of rank} \quad r-1$$

whose generating elements are ℓ^{x_i}th powers (for $i \geq 2$) of elements of $K^\times$ that do not depend on the x_i's. We proceed as above. We suppose that the entry $(1,1)$ of the submatrix is non-zero and has minimal ℓ-adic valuation (among the non-zero entries of its first $r-1$ columns), else we permute rows and columns of the original matrix (not the first row, and neither the first nor the last column) to achieve this condition, and rename the indices according to these swaps. Then the smallest d-parameter for H_{X_2} and a corresponding h-parameter are

$$\begin{aligned} d_2 &:= v_\ell\big(y(e_{11}e_{22} - e_{21}e_{12})\ell^{x_2}\big) \\ &= x_2 - v_\ell(e_{11}) + v_\ell(e_{11}e_{22} - e_{21}e_{12}) \qquad (6) \\ h_2 &:= v_\ell\Big(\operatorname{ord}\big(\zeta^{y(e_{11}f_2 - e_{21}f_1)\ell^{x_2}}\big)\Big) \\ &= \max\big(0, z - x_2 + v_\ell(e_{11}) - v_\ell(e_{11}f_2 - e_{21}f_1)\big). \qquad (7) \end{aligned}$$

We modify the matrix as above to have zeroes in the second column below the diagonal.

STEP k (for $3 \leq k \leq r$). Following this procedure, by iteration we find expressions for the functions $d_k, h_k, \delta_k, \epsilon_k$ of the desired form (up to permuting the indices, in their expressions we only find indices $i, j \leq k$).

At Step k we swap only rows and columns starting from the k-th ones, and we never affect the $(r+1)$-st column: the composition of these transpositions for the rows and for the columns is what we call σ_I and σ_J respectively. The assertion about determining σ follows from the fact that at the kth step the quantity that we want to be minimal is precisely the value that we take for d_k (by definition of d_k).

The first r columns of the final matrix form an upper triangular matrix. The integers d_k are in non-decreasing order (recall that d_1 was the smallest d--parameter) because the entries of the submatrix at Step k for $k \geq 2$ are integer combinations of entries of the submatrix at Step $k-1$ (which are either 0 or have ℓ-adic valuation at least d_{k-1}).

To conclude, we show that the d_k's and the h_k's are the divisibility parameters for H_X. The elements described by the rows of the final matrix are a basis $\gamma_1, \ldots, \gamma_r$ for a subgroup of H_X of index coprime to ℓ (which has the same divisibility parameters as H_X by Theorem 3.2). This is an ℓ-good basis by Lemma 4.1, and d_k, h_k are the divisibility parameters of γ_k by Lemma 2.1. □

REMARK 7. In the proof of Theorem 4.4 we transform a matrix, and at all steps the entries are integers of the following form: a function of the e_{ij}'s times ℓ^{x_k} for some k (the index k is the same for each row and different rows have different indices). We consider the non-zero entries of a submatrix and compare their ℓ-adic valuations. This amounts to selecting two non-zero entries at a time and considering inequalities of the type

$$x_{k_1} - x_{k_2} \leq f(e_{ij})$$

for some function f which depends only on the two entries that we are comparing, at which step we are in the algorithm, and on σ (if r is fixed, then there are only finitely many possibilities for the function f).

Proof of Theorem 1.1. This is a consequence of Theorem 4.4. □

Proof of Theorem 1.2. Given ℓ-divisibility parameters for the group

$$\left\langle \alpha_1^{\ell^{n-n_1}}, \ldots, \alpha_r^{\ell^{n-n_r}} \right\rangle$$

we can apply [1, Theorem 18] to compute the degree of (2). To compute the parameters we can apply Theorem 1.1 (setting $x_i := n - n_i$). □

5. The 2-divisibility parameters over $K(\zeta_4)$

Theorem 1.2 excludes the case $\ell = 2$ and $\zeta_4 \notin K$. If $\zeta_4 \notin K$, then in order to compute the degree of

$$K\big(\zeta_{2^m}, \sqrt[2^{n_1}]{\alpha_1}, \dots, \sqrt[2^{n_r}]{\alpha_r}\big)/K(\zeta_{2^m})$$

with $m \geq 2$ we may replace K with $K(\zeta_4)$ and apply Theorem 1.2 to compute the 2-divisibility parameters of the group

$$\left\langle \alpha_1^{2^{n-n_1}}, \dots, \alpha_r^{2^{n-n_r}} \right\rangle \quad \text{over } K(\zeta_4).$$

For $m = 1$ we can make use of [1, Lemma 19], which also requires the computation of degrees over $K(\zeta_4)$. In this section, we explain how the 2-divisibility parameters of a group change when extending K to $K(\zeta_4)$.

By [3] the 2-divisibility parameters of a finitely generated and torsion-free subgroup of $K^\times$ change from K to $K(\zeta_4)$ only if

$$K \cap \mathbb{Q}(\zeta_{2^\infty}) = \mathbb{Q}\big(\zeta_{2^s} + \zeta_{2^s}^{-1}\big) \tag{8}$$

holds for some $s \geq 2$. So we consider a number field K satisfying (8) and we set

$$f := \zeta_{2^s} + \zeta_{2^s}^{-1} + 2 = \zeta_{2^s}^{-1}(1 + \zeta_{2^s})^2 .$$

We also fix a torsion-free subgroup

$$G := \langle g_1, \dots, g_r \rangle$$

of $K^\times$ of rank r and set

$$H_X := \left\langle g_1^{2^{x_1}}, \dots, g_r^{2^{x_r}} \right\rangle,$$

where $X = (x_1, \dots, x_r)$ is an r-tuple of nonnegative integers.

Lemma 5.1. *The 2-divisibility parameters of H_X change from K to $K(\zeta_4)$ if and only if the same holds for G. Equivalently, H_X contains an element of the form $\pm(fa^2)^{2^d}$ for some $a \in K^\times$ and for some integer $d \geq 0$ if and only if G contains an element of such form.*

Proof. By [3, Theorem 1] the d-parameters for G (respectively, H_X) change from K to $K(\zeta_4)$ if and only if G (respectively, H_X) contains an element of the prescribed form. Since $H_X \subseteq G$, it is sufficient to prove that if G contains such an element, then so does H_X. Suppose that

$$\pm(fa^2)^{2^d} = \prod_{i=1}^{r} g_i^{e_i}$$

for some integers e_i. If w.l.o.g. we have $x := \max_i(x_i) \geq 1$, then H_X contains

$$(fa^2)^{2^{d+x}} = \prod_{i=1}^{r} (g_i^{2^{x_i}})^{e_i\, 2^{x-x_i}}\,. \qquad \square$$

For the remaining of the section suppose that G contains an element as in Lemma 5.1, so that the 2-divisibility parameters for H_X change from K to $K(\zeta_4)$. Let d_i, h_i be the d-parameters and h-parameters for H_X over K, see Theorem 4.4. By [3, Theorems 1 and 2] we have:

Remark 8. There is $j \in \{1, \ldots, r\}$ such that the d-parameters for H_X over $K(\zeta_4)$ are the d_i's for $i \neq j$ and $d_j + 1$, while the h-parameters for H_X over $K(\zeta_4)$ are the h_i's for $i \neq j$ and

$$\begin{aligned} h_j \quad & \text{if } d_j \geq s, \\ 0 \quad & \text{if } d_j = s-1 \quad \text{and} \quad h_j = 1, \\ 1 \quad & \text{if } d_j = s-1 \quad \text{and} \quad h_j = 0, \\ s - d_j \quad & \text{if } d_j \leq s-2. \end{aligned}$$

Theorem 5.2. *There is a finite procedure, not requiring computations over $K(\zeta_4)$, to determine formulas (involving only a finite case distinction) for the 2-divisibility parameters for H_X over $K(\zeta_4)$ for all X.*

Proof. We can express the elements g_i's in terms of strongly ℓ-independent elements $b_1, \ldots, b_r$ as in (5). By [3, Theorem 1 (3)] we may change the b_i's in such a way that one of them is of the form $\pm fa^2$ with $a \in K^\times$ (notice that any basis of $\langle b_1, \ldots, b_r \rangle$ consists of strongly ℓ-independent elements because the d-parameters are all zero).

The algorithm in the proof of Theorem 4.4 (which only requires a finite case distinction for the r-tuples X) yields a 2-good basis $\gamma_1, \ldots, \gamma_r$ of a subgroup H'_X of H_X of odd index having same 2-divisibility parameters as H_X over K (and over $K(\zeta_4)$) by Theorem 3.2. Notice that also H'_X contains an element of the form $\pm(fa^2)^{2^d}$. We may permute the indices i, j as in the proof of Theorem 4.4 and for every $n \in \{1, \ldots, r\}$ we write

$$\gamma_n = (-1)^{F_n} \cdot B_n^{2^{d_n}}, \qquad \text{where} \qquad B_n := \prod_{i \geq n} b_i^{y_{ni}}$$

for some integers y_{ni} and F_n, with y_{nn} odd, and where d_n is the d-divisibility parameter of γ_n (in particular, B_n is strongly 2-indivisible). To apply Remark 8

we can take as j any index such that B_j is of the form $\pm fa^2$. If there is no such index, let k be such that b_k is of the form $\pm fa^2$. Observe that (without using that b_k is of the special form) we can write

$$b_k c^2 = \prod_{i \in J} B_i \qquad \text{with} \qquad c \in K^\times$$

and

$$k \in J \subseteq \{k, \dots, r\}\,.$$

Let $j := \max J$ and consider the base change of H'_X which replaces γ_j by

$$\gamma'_j := \prod_{i \in J} \gamma_i^{2^{d_j - d_i}} = \pm \prod_{i \in J} B_i^{2^{d_j}} = \pm \big(f(ac)^2\big)^{2^{d_j}}\,,$$

see [3, Proof of Proposition 6]. The d-parameter of γ'_j is d_j, so again we have a 2-good basis. The d-parameter of γ'_j changes over $K(\zeta_4)$ so j is the index as in Remark 8. There we have to use the h-parameter of γ'_j, which is 0 unless $\sum F_i$ is odd, where the sum is over the indices $i \in J$ such that $d_i = d_j$. □

6. Three divisibility parameters

6.1. The case of rank 3

Let K be a number field, and let ℓ be a prime number. Let b_1, b_2, b_3 be strongly ℓ-independent elements in $K^\times$, fix some $\zeta \in \mu_K$ of order ℓ^z and let

$$g_i = \zeta^{f_i} \prod_{j=1}^{3} b_j^{e_{ij}}\,,$$

where for $i, j \in \{1, 2, 3\}$ we have integers e_{ij} such that the matrix (e_{ij}) has rank 3, and integers f_i such that $1 \le f_i \le \ell^z$. Thus $G = \langle g_1, g_2, g_3 \rangle$ is torsion-free and of rank 3.

We determine the ℓ-divisibility parameters for all groups of the form

$$H_X := \big\langle g_1^{\ell^{x_1}}, g_2^{\ell^{x_2}}, g_3^{\ell^{x_3}} \big\rangle\,,$$

where x_1, x_2, x_3 are non-negative integers. Consider the matrix of exponents associated to the given basis of H_X:

$$\left(\begin{array}{ccc|c} e_{11}\ell^{x_1} & e_{12}\ell^{x_1} & e_{13}\ell^{x_1} & f_1\ell^{x_1} \\ e_{21}\ell^{x_2} & e_{22}\ell^{x_2} & e_{23}\ell^{x_2} & f_2\ell^{x_2} \\ e_{31}\ell^{x_3} & e_{32}\ell^{x_3} & e_{33}\ell^{x_3} & f_3\ell^{x_3} \end{array}\right).$$

Up to reordering the b_j's and the g_i's (so up to reordering the rows and the columns of the matrix $(e_{ij}\ell^{x_i})$) we may suppose that

$x_1 + v_\ell(e_{11})$ is the minimum of
$$x_i + v_\ell(e_{ij}) \text{ for } i,j \in \{1,2,3\} \text{ (restricting to } e_{ij} \neq 0).$$

Similarly, denoting by Δ_{ij} the (i,j)th minor of the matrix (e_{ij}), we may suppose that

$x_2 + v_\ell(\Delta_{33})$ is the minimum of
$$x_2 + v_\ell(\Delta_{33}),\quad x_2 + v_\ell(\Delta_{32}),\quad x_3 + v_\ell(\Delta_{23}),\quad x_3 + v_\ell(\Delta_{22})$$
(restricting to $\Delta_{ij} \neq 0$).

The first two steps of the algorithm of the proof of Theorem 4.4 give the matrix
$$\left(\begin{array}{ccc|c} e_{11}\ell^{x_1} & e_{12}\ell^{x_1} & e_{13}\ell^{x_1} & f_1\ell^{x_1} \\ 0 & \Delta_{33}A_1\ell^{x_2} & \Delta_{32}A_1\ell^{x_2} & D_2A_1\ell^{x_2} \\ 0 & 0 & (\Delta_{22}\Delta_{33}-\Delta_{32}\Delta_{23})A_2\ell^{x_3} & (\Delta_{33}D_3-\Delta_{23}D_2)A_2\ell^{x_3} \end{array}\right),$$
where
$$D_i := e_{11}f_i - e_{21}f_1$$
are minors of the augmented matrix $(e_{ij} \mid f_i)$, and where
$$A_1 := \ell^{-v_\ell(e_{11})} \quad \text{and} \quad A_2 := \ell^{-v_\ell(e_{11}\Delta_{33})}.$$

Thus the d-parameters for H_X are
$$d_1 = x_1 + v_\ell(e_{11}),$$
$$d_2 = x_2 + v_\ell\left(\frac{\Delta_{33}}{e_{11}}\right),$$
$$d_3 = x_3 + v_\ell\left(\frac{\Delta_{22}\Delta_{33}-\Delta_{32}\Delta_{23}}{e_{11}\Delta_{33}}\right)$$
in non-decreasing order, and corresponding h-parameters are
$$h_1 = \max\bigl(0, z - x_1 - v_\ell(f_1)\bigr),$$
$$h_2 = \max\left(0, z - x_2 - v_\ell\left(\frac{D_2}{e_{11}}\right)\right),$$
$$h_3 = \max\left(0, z - x_3 - v_\ell\left(\frac{\Delta_{33}D_3-\Delta_{23}D_2}{e_{11}\Delta_{33}}\right)\right).$$

6.2. Three divisibility parameters

As observed in Theorem 4.4, the functions δ_k and ϵ_k do not depend on the rank. This means that for a (similarly defined) group of rank $r \geq 1$ the smallest d-parameter and corresponding h-parameters are d_1, h_1 as above, provided that

1. $x_1 + v_\ell(e_{11})$ is the minimum of $x_i + v_\ell(e_{ij})$ for $i, j \in \{1, \dots, r\}$ (restricting to the indices for which $e_{ij} \neq 0$).

For rank $r \geq 2$ the second smallest d-parameter and corresponding h-parameters are d_2, h_2 as above, provided that 1. holds and that

2. $x_1 + v_\ell\left(\dfrac{e_{11}e_{22} - e_{21}e_{12}}{e_{11}}\right)$ is the minimum of $x_1 + v_\ell\left(\dfrac{e_{11}e_{ij} - e_{i1}e_{1j}}{e_{11}}\right)$ for $i, j \in \{2, \dots, r\}$ (restricting to the indices for which $e_{11}e_{ij} - e_{i1}e_{1j} \neq 0$).

Finally, for rank $r \geq 3$ the third smallest d-parameter and a corresponding h-parameter are d_3, h_3 as above, provided that 1. and 2. hold and that, with the above notation,

3. $x_3 + v_\ell\left(\dfrac{\Delta_{22}\Delta_{33} - \Delta_{32}\Delta_{23}}{e_{11}\Delta_{33}}\right)$ is the minimum of $x_i + v_\ell\left(\dfrac{(e_{11}e_{ij} - e_{i1}e_{1j})(e_{11}e_{22} - e_{21}e_{12}) - (e_{11}e_{2j} - e_{21}e_{1j})(e_{11}e_{i2} - e_{i1}e_{12})}{e_{11}(e_{11}e_{22} - e_{21}e_{12})}\right)$ for $i, j \in \{3, \dots, r\}$ (restricting to the indices for which the integer inside the ℓ-adic valuation is non-zero).

The above conditions 1., 2., 3. hold up to permuting the rows and the columns of the original matrix, i.e., up to permuting the g_i's and the b_j's.

6.3. Example

Let $K = \mathbb{Q}(\zeta_3)$ and $\ell = 3$. Since the rational primes 2 and 5 are inert in K, they are strongly 3-independent in $K^\times$. Consider the group

$$G = \left\langle \zeta_3 2^3 5^9, 2^{27} 5 \right\rangle.$$

In order to minimize $v_3(e_{11})$ we let

$$b_1 = 5, \qquad b_2 = 2, \qquad g_1 = 2^{27}5, \qquad g_2 = \zeta_3 2^3 5^9$$

so that the augmented matrix of exponents becomes

$$\left(\begin{array}{cc|c} e_{11} & e_{12} & f_1 \\ e_{21} & e_{22} & f_2 \end{array}\right) = \left(\begin{array}{cc|c} 1 & 3^3 & 3 \\ 3^2 & 3 & 1 \end{array}\right).$$

The d-parameters for G are

$$d_1 := v_3(e_{11}) = 0$$

$$d_2 := v_3\left(\frac{e_{22}e_{11} - e_{12}e_{21}}{e_{11}}\right) = 1$$

and corresponding h-parameters are

$$h_1 := \max\bigl(0, 1 - v_\ell(f_1)\bigr) = 0,$$

$$h_2 := \max\left(0, 1 - v_\ell\left(\frac{e_{11}f_2 - e_{21}f_1}{e_{11}}\right)\right) = 1\,.$$

Consider now, for all non-negative integers x_1, x_2, the subgroup

$$H_X := \left\langle \left(2^{27}5\right)^{3^{x_1}},\, \left(2^3 5^9\right)^{3^{x_2}} \right\rangle \quad \text{of } G.$$

Its augmented matrix of exponents is

$$\left(\begin{array}{cc|c} 3^{x_1} & 3^{x_1+3} & 3^{x_1+1} \\ 3^{x_2+2} & 3^{x_2+1} & 3^{x_2} \end{array}\right).$$

If $x_1 \le x_2 + 1$, then we proceed as above and we get

$$d_1 = x_1, \qquad d_2 = x_2 + 1,$$

and

$$h_1 = 0, \qquad h_2 = \max(0, 1 - x_2)\,.$$

If $x_1 > x_2 + 1$, then we let instead

$$b_1 = 2, \qquad b_2 = 5, \qquad g_1 = \zeta_3 2^3 5^9, \qquad g_2 = 2^{27}5,$$

so that the matrix becomes

$$\left(\begin{array}{cc|c} 3^{x_2+1} & 3^{x_2+2} & 3^{x_2} \\ 3^{x_1+3} & 3^{x_1} & 3^{x_1+1} \end{array}\right)$$

and we have

$$d_1 = x_2 + 1, \qquad d_2 = x_1, \qquad \text{and} \qquad h_1 = \max(0, 1 - x_2), \qquad h_2 = 0\,.$$

REFERENCES

[1] DEBRY, C.—PERUCCA, A.: *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.

[2] PERUCCA, A.: *The order of the reductions of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.

[3] PERUCCA, A.—SGOBBA, P.—TRONTO, S.: *Addendum to: Reductions of algebraic integers [J. Number Theory **167** (2016), 259–283]*, J. Number Theory **209** (2020), 391–395.

[4] PERUCCA, A.—SGOBBA, P.—TRONTO, S.: *The degree of Kummer extensions of number fields*, Int. J. Number Theory **17** (2021), no. 5, 1091–1110.
DOI: `https://doi.org/10.1142/S1793042121500263`.

Received October 13, 2020
Accepted August 30, 2021

Antonella Perucca
Pietro Sgobba
Sebastiano Tronto
Department of Mathematics
Faculty of Science,
Technology and Medicine
University of Luxembourg
Avenue de la Fonte 6
L-4364 Esch-sur-Alzette
LUXEMBOURG

E-mail: antonella.perucca@uni.lu
pietro.sgobba@uni.lu
sebastiano.tronto@uni.lu